EXHIBIT C

Trials@uspto.gov
Tel: 571-272-7822

Paper 28
Date: October 5, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

MPH TECHNOLOGIES OY,
Patent Owner.

IPR2019-00821
Patent 8,037,302 B2

Before SALLY C. MEDLEY, KAMRAN JIVANI, and JOHN D. HAMANN, *Administrative Patent Judges.*

HAMANN, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining No Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

In this *inter partes* review, instituted pursuant to 35 U.S.C. § 314, Apple Inc. ("Petitioner") challenges the patentability of claims 1–16 ("the challenged claims") of U.S. Patent No. 8,037,302 B2 (Ex. 1001, "the '302 patent"), owned by MPH Technologies Oy ("Patent Owner"). We have jurisdiction under 35 U.S.C § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons discussed herein, we determine that Petitioner has not shown by a preponderance of the evidence that claims 1–16 are unpatentable.

II. BACKGROUND

A. Procedural History

Petitioner filed a Petition requesting *inter partes* review of the challenged claims of the '302 patent. Paper 1 ("Pet."). The Petition is supported by the Declaration of David Goldschlag, Ph.D. (Ex. 1003). Patent Owner filed a Preliminary Response. Paper 8.

We instituted *inter partes* review of all of the challenged claims of the '302 patent on all of the grounds raised in the Petition. Paper 9 ("Dec. on Inst."), 6–7, 31. Patent Owner filed a Response to the Petition. Paper 15 ("PO Resp."). The Response is supported by the Declaration of Professor George N. Rouskas, Ph.D. (Ex. 2002). Petitioner filed a Reply to Patent Owner's Response. Paper 18 ("Pet. Reply"). The Reply is supported by an additional Declaration of David Goldschlag, Ph.D. (Ex. 1020). Patent Owner filed a Sur-Reply to Petitioner's Reply. Paper 21 ("PO Sur-Reply").

An oral hearing was held on July 17, 2020. A transcript of the oral hearing is included in the record. Paper 27 ("Tr.").

B. Related Matter

The parties identify *MPH Techs. Oy v. Apple Inc.*, Case No. 4:18-cv-05935-PJH (N.D. Cal.), as a matter that may affect or would be affected by a decision in this proceeding. Pet. 2; Paper 7, 1.

C. The Challenged Patent (Ex. 1001)

The '302 patent relates to providing "secure connections in telecommunication networks" more efficiently. Ex. 1001, 1:13–14, 4:55–63, 7:3–5. In particular, the '302 patent relates to reducing the handover latency for secure connections, such as those employing Internet Protocol ("IP") Security ("IPSec") with mobile terminals[1] (i.e., terminals that can move from one network to another). *Id.* at 4:55–63, 7:3–5, 7:39–41.

According to the '302 patent, IPSec comprises a set of rules for "provid[ing] the capability to secure communications" between hosts. *Id.* at 1:38–39. These rules describe, *inter alia*, the concept of a Security Association ("SA"), which the '302 patent describes as "a one-way relationship between a sender and a receiver that offers [negotiated IPSec] security services to the traffic carried on it." *Id.* at 1:62–65. SAs are identified, in part, by the IP addresses of the hosts. *E.g.*, *id.* at 2:14–16. The '302 patent discloses that when a new SA is formed, "it is registered for immediate and/or later use" in a Security Association Database ("SAD"), "which is the nominal place to store IPSec SAs in the IPSec model." *Id.* at 7:45–53. Each host participating in the forming of the SA maintains a copy of the SAD, according to the '302 patent. *Id.* at 7:47–48.

[1] The '302 patent discloses that "the term[s] mobility and mobile terminal do[] not only mean physical mobility, . . . [but also] mean[] moving from one network to another, which can be performed by a physically fixed terminal as well." Ex. 1001, 3:51–55.

In addition, the '302 patent discloses that IPSec is intended to work with static network topologies. *Id.* at 3:19–22. For example, IPSec can secure communications between static hosts across a local area network ("LAN"), as well as across a private or public wide area network ("WAN"). *Id.* at 1:38–40. IPSec, however, "does not work well with mobile" terminals, according to the '302 patent, because when "a mobile terminal moves from one network to another [and changes addresses], an IPSec connection set up is required," which typically "is expensive in terms of latency," requiring "several seconds to complete." *Id.* at 4:52–60.

To address this problem, the '302 patent discloses avoiding the need, if possible, to set up an IPSec connection when the mobile terminal moves networks by relying on a SA that is already established. *E.g.*, *id.* at 10:39–43, 10:51–56. Figure 2, shown below, is a "signalling diagram," which describes the invention of the '302 patent. *Id.* at 9:5–6.

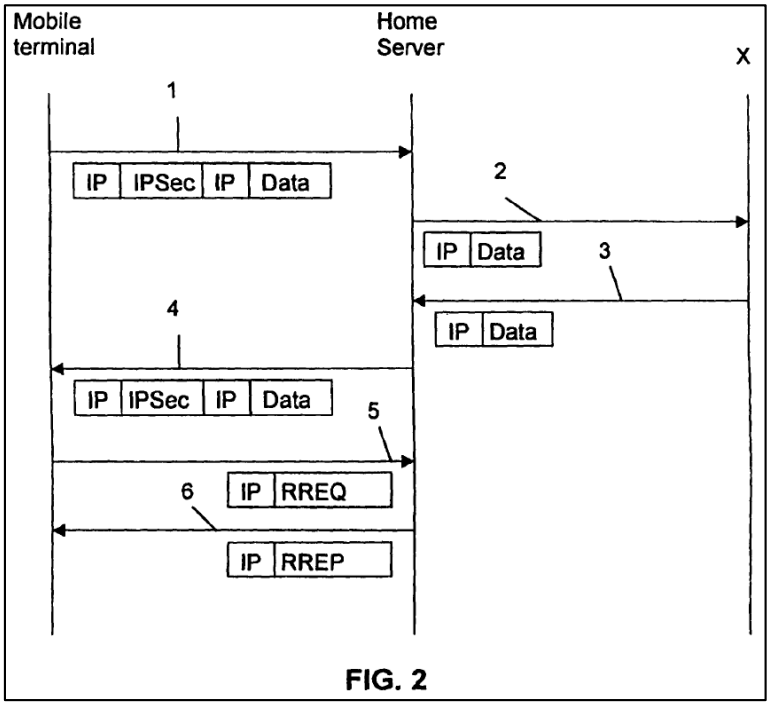

FIG. 2

Figure 2 "describes an example of the method of the invention for sending messages[, as shown in steps 1–6,] when a mobile terminal moves to a new address." *Id.* at 10:9–11. We focus on steps 1 and 5 between the mobile terminal and home server, because these are the illustrated steps relevant to our analysis below.

First, a SA is established between a first address of the mobile terminal and the address of the home server. *Id.* at 10:12–16. This SA is used to send a message from the mobile terminal to the home server, as illustrated in step 1. *Id.* at 10:21–25. Subsequently, the mobile terminal moves to a new network and obtains a new address from the new network. *Id.* at 10:39–40. "The mobile terminal then checks whether an SA . . . already exists between the new . . . address and the home server address. This check is normally done by inspecting the contents of" a SAD, "as specified by the IPSec protocol." *Id.* at 10:40–46.

If a SA between the mobile terminal's new address and the home server's address "already exists, this SA is registered to be the actual SA to be used." *Id.* at 10:51–56. Put differently, the SA is registered as an active connection (i.e., "a stored mobility binding that maps a given terminal address to one or more" SAs to determine to what address to forward packets). *E.g.*, *id.* at 8:13–14, 10:12–27. "This happens by means of a signalling message . . . done between the mobile terminal and the home server, described by step[] 5 . . . ." *Id.* at 10:57–59; *see also id.* at 7:59–63 (describing sending a Registration Request signalling message to register the actual connection to use). Alternatively, the '302 patent discloses that in lieu of a Registration Request, properly authenticated traffic from a new address can be used "as an implicit registration request, and a mobility

binding update [can be] performed automatically." *Id.* at 11:31–33. "When a[] . . . SA does not exist between the [mobile terminal's] new . . . address and the home server['s address], a[] . . . SA setup" occurs instead. *Id.* at 10:66–67.

D. The Challenged Claims

Petitioner challenges claims 1–16 of the '302 patent, of which claim 1 is the sole independent claim. Claim 1 is illustrative of the challenged claims and is reproduced below:

> 1. A method for ensuring secure forwarding of a message in a telecommunication network, comprising:
>
> providing a first terminal from which the message is sent and a second terminal to which the message is sent,
>
> a) establishing a first secure connection as being an active connection and extending between a first network address of the first terminal and an original network address of the second terminal, establishing a second secure connection extending between a second network address of the first terminal and the original network address of the second terminal,
>
> b) the first terminal changing from the first network address to the second network address, the first terminal checking whether the second secure connection already exists, and
>
> c) when the second secure connection already exists, the second terminal registering the already established second secure connection as being the active connection without having to reestablish the second secure connection.

Ex. 1001, 12:15–34.

E. Instituted Grounds of Unpatentability

We instituted trial based on the following grounds of unpatentability, which are all the grounds of unpatentability raised in the Petition:

	References	35 U.S.C.[2]	Challenged Claims
1.	Ahonen,[3] Ishiyama[4]	§ 103(a)	1–13, 16
2.	Ahonen, Ishiyama, Gupta[5]	§ 103(a)	14, 15

Pet. 3–4, 17–53.

III. LEVEL OF ORDINARY SKILL IN THE ART

To determine whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). In assessing the level of ordinary skill in the art, various factors may be considered, including the "type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field." *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (citing *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986)). "[O]ne or more factors may predominate." *Id.*

---

[2] The Leahy-Smith America Invents Act ("AIA") included revisions to 35 U.S.C. § 103 that became effective on March 16, 2013. Because the '302 patent issued from an application filed before March 16, 2013, we apply the pre-AIA version of the statutory basis for unpatentability.
[3] Int'l Pub. No. WO 01/54379 A1 (published July 26, 2001) (Ex. 1004).
[4] U.S. Patent No. 6,904,466 B1 (issued June 7, 2005) (Ex. 1005).
[5] Vipul Gupta *et al.*, *Complete Computing*, WWCA '98 PROC. 2D INT'L CONF. ON WORLDWIDE COMPUTING AND ITS APPLICATIONS (Mar. 4–5, 1998) (Ex. 1006).

In our Decision on Institution, we adopted Petitioner's proposed definition for one having ordinary skill in the art at the time of the invention of the '302 patent as one who would have had "a B.S. degree in Computer Science, Electrical Engineering, or an equivalent field, as well as at least 3–5 years of academic or industry experience in network security, or comparable industry experience." Dec. on Inst. 7 (citing Pet. 14; Ex. 1003 ¶ 22). Patent Owner does not dispute our adoption of Petitioner's definition, nor otherwise address the level of ordinary skill at the time of the invention of the '302 patent. *See generally* PO. Resp.; *see also* Ex. 2002 ¶ 24.

Because Petitioner's definition of the level of skill in the art is consistent with the '302 patent and the asserted prior art, we maintain Petitioner's definition for purposes of this Final Written Decision. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *GPAC*, 57 F.3d at 1579; *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978). We apply Petitioner's definition in our analysis below.

IV. CLAIM CONSTRUCTION

Because the Petition was filed after November 13, 2018, we construe the challenged claims by applying "the standard used in federal courts, in other words, the claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), which is articulated in *Phillips* [*v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc)]." *See* Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340, 51,340, 51,358 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018) (now codified at 37 C.F.R. § 42.100(b) (2019)). Under *Phillips*, the words of a claim are generally given their "ordinary and

customary meaning," which is the meaning they would have to a person of ordinary skill in the art at the time of the invention, in light of the specification and prosecution history. *See Phillips*, 415 F.3d at 1312–13.

The parties identify for construction "establishing a first secure connection" and "establishing a second secure connection," as recited in claim 1. Pet. 15–16; Prelim. Resp. 8–12. We address these terms in two parts (i.e., "secure connection" and "establishing"), as the parties do.

A. Secure Connection

In the Petition, Petitioner argued that a secure connection means "one or more . . . security associations." Pet. 15 (citing Ex. 1003 ¶¶ 40–43). In our Decision on Institution, we concluded that "we need not decide whether a 'secure connection' should be limited to one or more SAs[, but r]ather, it is sufficient that the parties do not dispute that a secure connection covers one or more SAs." Dec. on Inst. 9 (citations omitted). In the subsequent papers, the parties confirm that they do not dispute that a secure connection covers one or more SAs. Pet. Reply 3; PO Sur-Reply 2. Accordingly, we find that no express construction of "secure connection" is needed. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'").

B. Establishing

Patent Owner argues that "'**establishing** a first/second secure connection' requires **forming or creating a new** secure connection." PO Resp. 22; *see also id.* at 22–23 (citing Ex. 1001, 7:39–41, 7:45–48, 10:12–16, 12:19–25; Ex. 2002 ¶ 69). Petitioner agrees that "'[e]stablishing'

should be construed to mean 'forming or creating a new secure connection,' as proposed by" Patent Owner. Pet. Reply 4. We conclude that the '302 patent's Specification supports this proposed construction, and we construe "establishing a . . . secure connection" as meaning "forming or creating a new secure connection." *See* Ex. 1001, code (57), 7:13–15, 7:39–41, 10:12–16.

V. PRINCIPLES OF LAW

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time of the invention to a person having ordinary skill in the art. *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of non-obviousness, if present.[6] *See Graham*, 383 U.S. at 17–18. When evaluating a claim for obviousness, we also must "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

VI. ALLEGED OBVIOUSNESS OVER AHONEN AND ISHIYAMA

Petitioner argues that the combination of Ahonen and Ishiyama renders claims 1–13 and 16 of the '302 patent obvious under 35 U.S.C.

[6] Patent Owner does not present arguments or evidence of such objective evidence of non-obviousness in its Response. *See generally* PO Resp.

§ 103(a). Pet. 17–50. We have reviewed the parties' arguments and the evidence of record. For the reasons that follow, we determine that Petitioner does not show by a preponderance of the evidence that claims 1–13 and 16 would have been obvious to one of ordinary skill in the art in view of Ahonen and Ishiyama.

A. Summary of Ahonen

Ahonen relates to a virtual private network ("VPN") "in which a mobile terminal establishes a secure connection with a correspondent host located in an intranet, via a [s]ecurity [g]ateway" (also known as a firewall). Ex. 1004, 3:5–7. Figure 1, shown below as annotated by Petitioner, illustrates this network topology, in accordance with Ahonen's invention. *Id.* at 7:1–2.

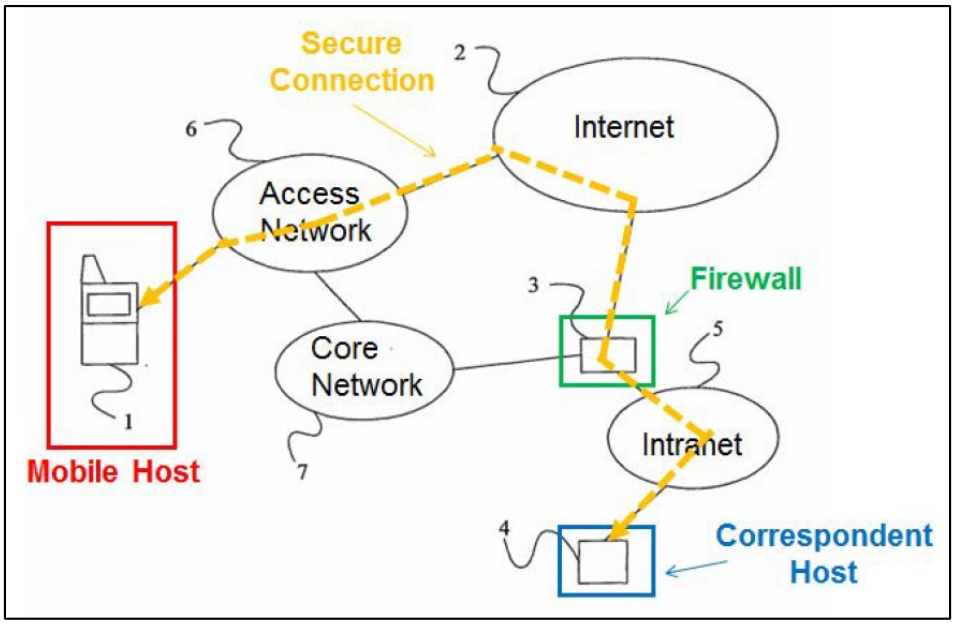

Figure 1 illustrates mobile host 1 connected to correspondent host 4 via access network 6, Internet 2, firewall 3, and intranet 5. *Id.* at 7:23–27. As annotated by the dotted line, a secure connection is established between mobile host 1 and correspondent host 4 over this path. *Id.* at 7:28–31.

Thereafter, mobile host 1 sends firewall 3 an authentication certificate, which contains, *inter alia*, the identity of the SA to use for subsequent communication between mobile host 1 and correspondent host 4. *E.g.*, *id.* at code (57). Mobile host 1 can then send data packets to correspondent host 4 using the identified SA, via firewall 3. *Id.* However, firewall 3 only forwards the data packets to correspondent host 4 if they are authenticated by firewall 3. *Id.*

Ahonen discloses that IPSec can be used to create the secure connection between mobile host 1 and correspondent host 4. *Id.* at 3:19–20. "In the IP[S]ec model[,however,] the end points of the secure connection are identified by their IP addresses." *Id.* at 3:21–22. "Whilst this may be satisfactory for users having a fixed connection, [according to Ahonen,] it . . . present[s] problems for the mobile user . . . who wishes to roam [because] . . . the IP address allocated to the roaming mobile user is likely to change" as the user moves between networks. *Id.* at 3:22–26. According to Ahonen, when an IP address changes, it is difficult to reuse the pre-existing SAs, and the communicating parties may need to establish new SAs using the new IP address. *Id.* at 3:26–29. "This will result in increased signalling traffic and will degrade the performance of the VPN . . . ." *Id.* at 3:30–31.

To address this problem, Ahonen's invention discloses "reduc[ing] the amount of security related messaging during on-the-fly IP address changes, as the SAs needed to provide for secure communication between the mobile host and the correspondent host pre-exist." *Id.* at 4:30–32. More specifically, Ahonen discloses negotiating one or more IPSec SAs between mobile host 1 and correspondent host 4 in preparation for providing future secure connections more efficiently when mobile host 1 roams. *E.g.*, *id.* at

5:31–6:1, 8:2–5, 8:28–9:2, 15:1–3. Ahonen discloses that the "[d]etails of the negotiated SAs are held at . . . firewall [3] in a Security Association Database (SAD)" on "the external side interface," so that the mobile host can use the pre-existing SAs when roaming. *Id.* at 15:4–9.

More specifically, Ahonen discloses that when mobile host 1 roams, it can "remotely 'activate' [the] pre-existing secure connections to . . . correspondent host 4." *Id.* at 16:16–19. In particular, Ahonen discloses, to activate a pre-existing connection, mobile host 1 sends to firewall 3 an authorization certificate, which includes: (i) "the (New) Source and Destination IP addresses (if changed),"[7] (ii) the cookies used to negotiate the SAs between mobile host 1 and correspondent host 4, (iii) the IPSec protocol ID, and (iv) the Security Parameter Index ("SPI") of the SA. *Id.* at 17:1–11. Firewall 3 searches its Remote Control DataBase ("RCDB") for records matching the authorization certificate's cookies, IPSec protocol ID, and SPI. *Id.* at 17:19–25. If a match is found, firewall 3 sends an acknowledgement back to mobile host 1. *Id.* at 18:3–4. In addition, Ahonen discloses that if the source IP address was changed, firewall 3 also will "forward the new Source and Destination IP addresses to the correspondent host 4." *Id.* at 18:7–8. Ahonen discloses that correspondent host 4 then modifies "its SAD database to correctly reflect the change of the mobile host's IP address to the new valid one." *Id.* at 18:10–12.

[7] Ahonen discloses that "mobile host 1 might be required to use a new IP address when communicating via" the visited access network. Ex. 1004, 16:22–24.

B. Summary of Ishiyama

Ishiyama relates to improving a mobile computer's "capab[ility] of carrying out communications while moving among a plurality of inter-connected networks." Ex. 1005, 1:9–11. In furtherance of this mobility, Ishiyama discloses having the mobile computer send a notification to its correspondent host when the mobile computer moves networks and gets a new address. *E.g.*, *id.* at 3:63–67, 6:13–18, 15:37–16:10.

According to one aspect of Ishiyama's invention for an IPSec embodiment, Ishiyama discloses that when transmitting a packet, the mobile computer's IPSec module "first searches through a security policy database" ("SPD"), using appropriate elements such as the source/destination address of a packet, to select a security policy, which identifies a SA to use to transmit the packet. *Id.* at 8:9–11, 9:50–54, 10:1–13.

C. Challenged Claim 1

Claim 1 recites, *inter alia*, "establishing a first secure connection as being an active connection and extending between a first network address of the first terminal and an original network address of the second terminal." Ex. 1001, 12:19–22. Petitioner relies on Ahonen for teaching this limitation. Pet. 27–38. We agree with Patent Owner and find that Ahonen fails to teach this limitation. PO Resp. 48–52; PO Sur-Reply 20–21.

This limitation has two requirements in establishing a first secure connection, namely, that the secure connection is established (i) as "extending between a first network address of the first terminal and an original network address of the second terminal" and (ii) "as being an active connection." In accordance with our above construction, the first requirement is met by "forming or creating a new secure connection"

between the claimed addresses. *See supra* Section IV(B) (construing establishing a secure connection).

As to the second requirement, the '302 patent teaches that "[w]hen a new secure connection is formed, it is registered for immediate and/or later use." Ex. 1001, 7:45–46. The '302 patent uses the phrases "for immediate use" and being "active" interchangeably. *See, e.g.*, *id.* at code (57), 7:16–20, 7:59–63, 8:12–26, 10:54–55. For example, the '302 patent teaches that "[t]he actual connection(s) to be used is registered." *Id.* at 7:59–63. In more detail, the '302 patent teaches that "[t]he active SA is a stored mobility binding that maps a given terminal address to one or more IPSec tunnel mode SAs," and that "[t]he mobility binding is necessary, . . . [because t]here has to be some way for the first terminal to determine which security association(s) to actually use when processing packets." *Id.* at 8:12–15, 8:23–27. Accordingly, the '302 patent teaches that "[w]hen a new secure connection is formed, it is registered" as being (i) an active connection or (ii) for later use. *Id.* at 7:45–46, 8:12–15, 8:23–27. Here, the claim language requires that when the first secure connection is established, it is registered as being an active connection. *Id.* at 12:19–22.

In addition, Dr. Rouskas' following declaration testimony is consistent with our conclusions:

> Based on the language of the claim, and the '302 Patent's disclosure that "[w]hen a new secure connection is formed, it is **registered for immediate and/or later use**," Ex. 1001[,7:45–46], a POSITA would understand "establishing a first secure connection **as being an active connection**" to mean that the first secure connection is established as an active connection for immediate use, as opposed to an inactive connection reserved for later use. Therefore, as any POSITA would have understood, this term not only requires creating or forming a new secure

> connection, but also creating or forming a new secure connection as being an **active** connection.

Ex. 2002 ¶ 111. We find that this testimony is consistent with the plain and ordinary meaning of the limitation's claim language and the '302 patent's Specification. Ex. 1001, 7:13–16, 7:39–46, 12:19–22.

We are not persuaded by Petitioner's arguments that "nothing in the claims or the [S]pecification requires an element of 'immediacy' or a particular timing to exist in the claims." Pet. Reply 16–17 (citing Ex. 1020 ¶¶ 39–42). Rather, the plain language of the limitation requires that when the first secure connection is established (i.e., when forming or creating a new first secure connection), it also is registered as being an active connection at that time. More specifically, the claim language recites "establishing a first secure connection as being an active connection," and hence, tethers the timing of registering the connection as an active connection to when the secure connection is formed. Ex. 1001, 12:19–22. Notably, claim 1 also recites "establishing a second secure connection," but without reciting that it is established as being an active connection. *Id.* at 12:22–25. Rather, claim 1 requires "registering the already established second secure connection as being the active connection," after the first terminal changes to a second address associated with the second secure connection. *Id.* at 12:30–32. Hence, claim 1 clearly provides particular timing with respect to when secure connections are made active, including that the first secure connection is made active when the first secure connection is established. *Id.* at 12:15–34.

Furthermore, the '302 patent's Specification supports that when the first secure connection is established (i.e., when forming or creating a new

first secure connection), it also is registered as being an active connection at that time. Specifically, the Specification teaches that "[*w*]*hen* a new secure connection is formed, it is registered for immediate and/or later use." *Id.* at 7:45–46 (emphasis added); *see also id.* at code (57), 7:16–20, 7:59–63, 8:12–26, 10:54–55 (using "active" and "for immediate use" interchangeably).

We also find that Petitioner mischaracterizes Patent Owner's argument as "'establishing . . . as being an active connection,' means the connection must be used 'immediately' as it is established, or in other words: 'concurrently.'" Pet. Reply 16 (citing PO Resp. 49). Petitioner conflates establishing a connection "as being an active connection," with actual use of the connection. *Id.*; *see also id.* n.2 (arguing that "if something cannot be used 'later' it must be used 'now' or 'concurrently'"). Rather, as Patent Owner argues, being an active connection means that the connection is available "*for* immediate use." PO Resp. 49 (emphasis added). *For* immediate use does not mean that the connection actually must be used at that time. Ex. 1001, code (57), 7:16–20, 7:59–63, 8:12–26, 10:54–55.

We also are not persuaded by Petitioner's arguments that "[a]t most, the 'active connection' element simply means that the 'secure connection' *can* be used by the mobile host after it is established," but "[t]here is no limitation on when that use needs to occur—and it certainly need not be 'immediate.'" Pet. Reply 17 (citing Ex. 1020 ¶ 40). Again, a secure connection being established as an active connection (i.e., being available for immediate use when the secure connection is formed) does not require immediate use. Rather, as Petitioner acknowledges, the secure connection

"*can* be used by the mobile host." *Id.*; Ex. 1001, code (57), 7:16–20, 7:59–63, 8:12–26, 10:54–55.

We also are not persuaded by Petitioner's arguments that "a suggestion that the claims require a connection to be 'established' and concurrently/immediately 'active' would defy the laws of physics and computer processing." Pet. Reply 17 (citing Ex. 1020 ¶ 41). Put differently, Petitioner argues that "[c]omputers function in specific step-by-step orders and do not perform operations 'immediately' or 'simultaneously,'" and thus, "the claims cannot be read to exclude the creation of an SA ***before*** the activation of an SA in view of how technology operates." *Id.* (citing Ex. 1020 ¶¶ 41–42). We find that these arguments are inapposite. Neither claim 1, nor the Specification, suggests that a secure connection is created and made active in simultaneous computer functions. *See, e.g.*, Ex. 1001, 7:13–16, 7:39–46, 12:19–22. Rather, claim 1 requires, and the Specification teaches, that when the first secure connection is established, it is registered as being an active connection. *See supra*; Ex. 1001, 7:45–46, 12:19–22. This timing does not preclude the secure connection being formed before the connection is made active as part of establishing the secure connection. *Id.* Again, "[*w*]*hen* a new secure connection is formed, it is registered for immediate and/or later use." *Id.* at 7:45–46 (emphasis added).

We have considered Dr. Goldschlag's testimony about the meaning of this limitation, but we accord it little weight because it is contrary to the plain claim language and the Specification's teachings, and is without sufficient factual corroboration. *See* Ex. 1020 ¶¶ 39–43; Ex. 1001, 7:13–16, 7:39–46, 7:45–46, 12:19–22; *see also In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1368 (Fed. Cir. 2004) ("[T]he Board is entitled to weigh the

declarations and conclude that the lack of factual corroboration warrants discounting the opinions expressed in the declarations."); 37 C.F.R § 42.65(a).

As to Ahonen's disclosure, we agree with Patent Owner and find that Ahonen fails to teach "establishing a first secure connection as being an active connection and extending between a first network address of the first terminal and an original network address of the second terminal." Ex. 1001, 12:19–22. More specifically, for the reasons we provide below, Ahonen fails to teach that the first secure connection is registered as being an active connection when the first secure connection is formed.

Petitioner argues that Ahonen discloses this limitation. Pet. 30–32. More specifically, Petitioner argues that Ahonen discloses establishing multiple secure connections (i.e., IPSec SAs) between mobile host 1 (i.e., the first terminal) and correspondent host 4 (i.e., the second terminal) "during a 'preparations' phase." *Id.* at 30 (citing Ex. 1004, 8:28–30, 8:32–9:2, 15:1–3); Pet. Reply 18 (citing Ex. 1004, 8:27–9:6, 13:20–28). According to Petitioner, "Ahonen further explains that during this very same preparations function, each of the SAs are activated." Pet. Reply 18 (citing Ex. 1004, 13:20–23, 15:11–16:14). In particular, Petitioner argues that "Ahonen explains that as a part of the preparations function, the mobile host sends an 'authorisation certificate' which enables the firewall to serve the mobile host." *Id.* (citing Ex. 1004, 15:11–16:14; Ex. 1020 ¶¶ 43–44). "Upon receiving the 'authorisation certificate,' 'firewall 3 is now *ready to serve the mobile host* 1 and the correspondent host 4 traffic via the Remote Control function,'" according to Petitioner. *Id.* (quoting Ex. 1004, 16:9–10; citing Ex. 1020 ¶ 45). Petitioner argues that "[t]his description explicitly teaches

that Ahonen's activation of a secure connection is part of and occurs *during* (*i.e.*, immediate use) the preparations function, which is when . . . the 'first secure connection' is 'established.'" *Id.* (citing Ex. 1020 ¶¶ 43–45).

We disagree with Petitioner that Ahonen teaches making a secure connection active as part of, or during, the preparations function. To the contrary, Ahonen teaches providing to the firewall information about the SAs created during the preparations function so that a mobile host later can remotely activate the SAs. Ex. 1004, 15:11–16:17. More specifically, Ahonen teaches that "[t]o conclude the preparations function, the mobile host 1 will send a specific formatted authorisation certificate to the firewall 3," containing "at least a formatted list of identities of the phase 2 SAs that were pre-created." *Id.* at 15:11–15. "The contents of the received authorisation certificates are stored in a . . . RCDB[], within the firewall 3." *Id.* at 16:4–5. Ahonen teaches that after receiving and storing this information, the firewall 3 "now is ready to serve the mobile host 1 and the correspondent host 4 traffic *via the Remote Control function*." *Id.* at 16:9–10 (emphasis added). Notably, Ahonen explicitly teaches that the firewall being "now . . . ready to serve" is in reference to the remote control function. *Id.* The remote control function occurs after the preparations function has concluded, and "is used by the mobile host 1 to remotely 'activate' preexisting secure connections to the correspondent host 4." *Id.* at 15:11–13, 16:16–17. For example, "[i]f the mobile host user travels away from the intranet 5, the SAs which were created during the preparations function stage can be brought into use" via the remote control function. *Id.* at 16:17–19.

In addition, Ahonen teaches that the information about each of the pre-created SAs sent to the firewall 3 can include "a Remote Control flag indicating whether this SA has been 'activated' by the mobile host 1 from outside of the intranet 5," and that "[i]nitially, in the Informational certificate, this flag is set to 'Off' which means that the corresponding phase 2 SA has not been activated by the Remote Control function." *Id.* at 15:15–16, 15:31–16:2. In contrast, Ahonen teaches that "the Remote Control flag is set to 'On'" after the firewall 3 receives a subsequent control authorisation certificate from mobile host 1, and identifies a matching record in the RCDB. *Id.* at 17:1–32 (describing the operation of the remote control function). These teachings from Ahonen further support that the pre-created SAs are not made active in the preparations function because the Remote Control flag is initially set to "Off," and not changed to "On" until remotely activated by a mobile host. *Id.* at 15:15–16:32.

Also, we accord Dr. Goldschlag's testimony on Ahonen teaching this limitation little, if any, weight. *See* Ex. 1020 ¶¶ 43–45. Dr. Goldschlag's opinions are contrary to Ahonen's teachings, which we discuss above.

Lastly, any statements in the Decision on Institution regarding the sufficiency of Petitioner's showings for this limitation were preliminary. *See Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1068 (Fed. Cir. 2016) ("At th[e Institution] point, the Board is considering the matter preliminarily without the benefit of a full record. The Board is free to change its view of the merits after further development of the record . . . ."). Upon a review of the full record, we find that Petitioner's showing for this limitation is insufficient for the reasons we provide above.

In summary, we find that Petitioner fails to show that the combination of Ahonen and Ishiyama teaches "establishing a first secure connection as being an active connection and extending between a first network address of the first terminal and an original network address of the second terminal." Accordingly, we find that Petitioner fails to show by a preponderance of the evidence that the combination of Ahonen and Ishiyama renders claim 1 obvious.

D. Challenged Claims 2–13 and 16

Claims 2–13 and 16 depend, directly or indirectly, from independent claim 1, and thus, incorporate claim 1's limitations. Ex. 1001, 12:15–67, 14:1–3. As we discuss above, Petitioner fails to show that the combination of Ahonen and Ishiyama teaches a limitation of claim 1. And, Petitioner's arguments with respect to claims 2–13 and 16 do not remedy this deficiency. Pet. 38–50. Accordingly, we find that Petitioner fails to show by a preponderance of the evidence that the combination of Ahonen and Ishiyama renders claims 2–13 and 16 obvious.

VII. ALLEGED OBVIOUSNESS OVER AHONEN, ISHIYAMA, AND GUPTA

Petitioner argues that the combination of Ahonen, Ishiyama, and Gupta renders claims 14 and 15 obvious. Pet. 50–53. Claims 14 and 15 depend from independent claim 1, and thus, incorporate claim 1's limitations. Ex. 1001, 13:1–7. As we discuss above, Petitioner fails to show that the combination of Ahonen and Ishiyama teaches a limitation of claim 1. Petitioner's arguments with respect to claims 14 and 15 and Gupta's teachings do not remedy the deficiencies discussed above with respect to claim 1. Pet. 50–53. Accordingly, we find that Petitioner fails to

show by a preponderance of the evidence that the combination of Ahonen, Ishiyama, and Gupta renders claims 14 and 15 obvious.

VIII. CONCLUSION

Based on the full record before us, we determine that Petitioner has not shown by a preponderance of the evidence that (i) claims 1–13 and 16 of the '302 patent are unpatentable under 35 U.S.C. § 103(a) over the combination of Ahonen and Ishiyama, and (ii) claims 14 and 15 of the '302 patent are unpatentable under 35 U.S.C. § 103(a) over the combination of Ahonen, Ishiyama, and Gupta.

Claim(s)	**35 U.S.C §**	**Reference(s)/Basis**	**Claims Shown Unpatentable**	**Claims Not Shown Unpatentable**
1–13, 16	103(a)	Ahonen, Ishiyama		1–13, 16
14, 15	103(a)	Ahonen, Ishiyama, Gupta		14, 15
Overall Outcome				1–16

IX. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), Petitioner has not shown by a preponderance of the evidence that claims 1–16 of the '302 patent are unpatentable; and

FURTHER ORDERED that parties to the proceeding seeking judicial review of this Final Written Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2019-00821
Patent 8,037,302 B2

PETITIONER:

Michael D. Specht
Daniel S. Block
Keyur P. Parikh
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
mspecht-ptab@sternekessler.com
dblock-ptab@sternekessler.com
kparikh-ptab@sternekessler.com

PATENT OWNER:

James T. Carmichael
Stephen Schreiner
CARMICHAEL IP LAW, PLLC
jim@carmichaelip.com
schreiner@carmichaelip.com

Christopher J. Lee
Richard B. Megley
Brian E. Haan
Ashley E. LaValley
LEE SHEIKH MEGLEY & HAAN LLC
clee@leesheikh.com
rmegley@leesheikh.com
bhaan@leesheikh.com
alavalley@leesheikh.com

Kenneth J. Weatherwax
Patrick Maloney
Jason C. Linger
LOWENSTEIN & WEATHERWAX LLP
weatherwax@lowensteinweatherwax.com
maloney@lowensteinweatherwax.com
linger@lowensteinweatherwax.com